

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Hideyuki SUZUKI, et al.

GAU:

SERIAL NO: New Application

EXAMINER:

FILED: Herewith

FOR: WIRELESS COMMUNICATION SYSTEM, TERMINAL, PROCESSING METHOD FOR USE IN THE
TERMINAL, AND PROGRAM FOR ALLOWING THE TERMINAL TO EXECUTE THE METHOD

REQUEST FOR PRIORITY

COMMISSIONER FOR PATENTS
ALEXANDRIA, VIRGINIA 22313

SIR:

- ☐ Full benefit of the filing date of U.S. Application Serial Number _____, filed _____, is claimed pursuant to the provisions of 35 U.S.C. §120.
- ☐ Full benefit of the filing date(s) of U.S. Provisional Application(s) is claimed pursuant to the provisions of 35 U.S.C. §119(e):
Application No. _____ Date Filed _____

☒ Applicants claim any right to priority from any earlier filed applications to which they may be entitled pursuant to the provisions of 35 U.S.C. §119, as noted below.

In the matter of the above-identified application for patent, notice is hereby given that the applicants claim as priority:

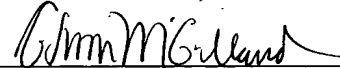
<u>COUNTRY</u>	<u>APPLICATION NUMBER</u>	<u>MONTH/DAY/YEAR</u>
Japan	2003-059359	March 6, 2003

Certified copies of the corresponding Convention Application(s)

- ☒ are submitted herewith
- ☐ will be submitted prior to payment of the Final Fee
- ☐ were filed in prior application Serial No. _____ filed _____
- ☐ were submitted to the International Bureau in PCT Application Number _____
Receipt of the certified copies by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.
- ☐ (A) Application Serial No.(s) were filed in prior application Serial No. _____ filed _____; and
- ☐ (B) Application Serial No.(s) _____
- ☐ are submitted herewith
- ☐ will be submitted prior to payment of the Final Fee

Respectfully Submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.



Bradley D. Lytle

Registration No. 40,073

Customer Number

22850

Tel. (703) 413-3000
Fax. (703) 413-2220
(OSMMN 05/03)

C. Irvin McClelland
Registration Number 21,124

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 3 年 3 月 6 日
Date of Application:

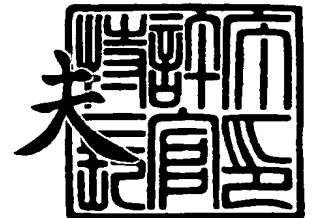
出 願 番 号 特 願 2 0 0 3 - 0 5 9 3 5 9
Application Number:
[ST. 10/C] : [J P 2 0 0 3 - 0 5 9 3 5 9]

出 願 人 ソニー株式会社
Applicant(s):

2 0 0 3 年 1 2 月 1 6 日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康 夫



【書類名】 特許願

【整理番号】 0390099014

【提出日】 平成15年 3月 6日

【あて先】 特許庁長官殿

【国際特許分類】 H04L 9/32

【発明者】

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
内

【氏名】 鈴木 英之

【発明者】

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
内

【氏名】 齋藤 真

【特許出願人】

【識別番号】 000002185

【氏名又は名称】 ソニー株式会社

【代理人】

【識別番号】 100112955

【弁理士】

【氏名又は名称】 丸島 敏一

【手数料の表示】

【予納台帳番号】 172709

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 0206900

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 無線通信システム、端末、その端末における、無線方法並びにその方法を端末に実行させるためのプログラム

【特許請求の範囲】

【請求項 1】 複数の端末により構成される無線通信システムであって、
端末権限認証証明書の種類を識別する識別子を有するビーコン情報を含む信号を送信する第 1 の端末と、

前記信号に応答して前記識別子に合致する種類の端末権限認証証明書を提示して前記第 1 の端末に対して認証を要求する第 2 の端末と
を具備することを特徴とする無線通信システム。

【請求項 2】 複数の端末により構成される無線通信システムであって、
当該端末における動作モードを示すビーコン情報を含む信号を送信する第 1 の端末と、

前記信号に応答して前記前記第 1 の端末における動作モードと自端末における動作モードとが一致している場合に、前記自端末における動作モードに関する権限を示す端末権限認証証明書を提示して前記第 1 の端末に対して認証を要求する第 2 の端末と

を具備することを特徴とする無線通信システム。

【請求項 3】 自端末のアクセス権限を示す端末権限認証証明書を格納する端末権限認証証明書テーブルと、

端末権限認証証明書の種類を識別する識別子を有するビーコン情報を含む信号を他の端末から受信するための受信手段と、

前記端末権限認証証明書テーブルに保持された端末権限認証証明書のうち前記受信手段により受信された信号に含まれる前記識別子に合致するものを提示して前記他の端末に対して自端末の認証を要求する認証要求手段と
を具備することを特徴とする端末。

【請求項 4】 前記端末権限認証証明書の種類を識別する識別子は、当該端末権限認証証明書を発行した端末の端末識別子であることを特徴とする請求項 3 記載の端末。

【請求項 5】 端末権限認証証明書発行端末の公開鍵証明書を保持する端末権限認証証明書発行端末リストテーブルと、

前記認証要求手段による認証要求に応答して前記他の端末が要求する第 2 の認証要求を受信する認証要求受信手段と、

この認証要求受信手段が受信した前記第 2 の認証要求に含まれる第 2 の端末権限認証証明書を前記端末権限認証証明書発行端末リストテーブルに保持された公開鍵証明書に含まれる公開鍵によって検証する検証手段と
をさらに具備することを特徴とする請求項 3 記載の端末。

【請求項 6】 前記端末権限認証証明書の種類を識別する識別子は、当該端末権限認証証明書を発行した端末の端末識別子であり、

前記端末権限認証証明書発行端末リストテーブルは、前記端末権限認証証明書を発行した端末の端末識別子と、前記端末権限認証証明書を発行した端末の公開鍵証明書と、前記端末権限認証証明書の前記端末権限認証証明書テーブルにおける格納位置とを関連付けて記憶すること
を特徴とする請求項 5 記載の端末。

【請求項 7】 自端末のアクセス権限を示す端末権限認証証明書を保持する端末権限認証証明書テーブルと、

この端末権限認証証明書テーブルにおける端末権限認証証明書の種類を識別する識別子を有するビーコン情報を含む信号を他の端末に対して送信する送信手段と
を具備することを特徴とする端末。

【請求項 8】 前記端末権限認証証明書の種類を識別する識別子は、当該端末権限認証証明書を発行した端末の端末識別子である
ことを特徴とする請求項 7 記載の端末。

【請求項 9】 自端末のアクセス権限を示す端末権限認証証明書を複数保持する端末権限認証証明書テーブルと、

この端末権限認証証明書テーブルにおける複数の端末権限認証証明書から一つの端末権限認証証明書を選択するよう促す選択手段と、

この選択手段において選択された端末権限認証証明書の種類を識別する識別子

を有するビーコン情報を含む信号を他の端末に対して送信する送信手段とを具備することを特徴とする端末。

【請求項 10】 前記端末権限認証証明書の種類を識別する識別子は、当該端末権限認証証明書を発行した端末の端末識別子であることを特徴とする請求項 9 記載の端末。

【請求項 11】 自端末のアクセス権限を示す端末権限認証証明書を格納する端末権限認証証明書テーブルと、

自端末の動作モードを含む状態テーブルと、

他の端末の動作モードを有するビーコン情報を含む信号を当該他の端末から受信するための受信手段と、

前記自端末の動作モードと前記他の端末の動作モードとが合致する場合に前記端末権限認証証明書テーブルに保持された端末権限認証証明書を提示して前記他の端末に対して自端末の認証を要求する認証要求手段とを具備することを特徴とする端末。

【請求項 12】 端末権限認証証明書発行端末の公開鍵証明書を保持する端末権限認証証明書発行端末リストテーブルと、

前記認証要求手段による認証要求に応答して前記他の端末が要求する第 2 の認証要求を受信する認証要求受信手段と、

この認証要求受信手段が受信した前記第 2 の認証要求に含まれる第 2 の端末権限認証証明書を前記端末権限認証証明書発行端末リストテーブルに保持された公開鍵証明書に含まれる公開鍵によって検証する検証手段と、

前記検証に成功した場合において前記第 2 の端末権限認証証明書に含まれる可能動作モードによって前記他の端末の動作モードが許容されていなければ前記第 2 の認証要求は失敗したものとする動作モード確認手段とをさらに具備することを特徴とする請求項 11 記載の端末。

【請求項 13】 前記端末権限認証証明書の種類を識別する識別子は、当該端末権限認証証明書を発行した端末の端末識別子であり、

前記端末権限認証証明書発行端末リストテーブルは、前記端末権限認証証明書を発行した端末の端末識別子と、前記端末権限認証証明書を発行した端末の公開

鍵証明書と、前記端末権限認証証明書の前記端末権限認証証明書テーブルにおける格納位置とを関連付けて記憶することを特徴とする請求項 1 2 記載の端末。

【請求項 1 4】 前記他の端末との間で使用する管理ポリシーを保持するポリシーテーブルと、

前記動作モード確認手段によって第 2 の認証要求に失敗したものとされなかった場合には前記第 2 の端末権限認証証明書に含まれる管理ポリシーを前記ポリシーテーブルに設定する管理ポリシー設定手段と
をさらに具備することを特徴とする請求項 1 2 記載の端末。

【請求項 1 5】 自端末の動作モードを含む状態テーブルと、

前記自端末の動作モードを有するビーコン情報を含む信号を他の端末に対して送信する送信手段と
を具備することを特徴とする端末。

【請求項 1 6】 自端末のアクセス権限を示す端末権限認証証明書を格納する端末権限認証証明書テーブルと、

自端末の動作モードを含む状態テーブルと、

端末権限認証証明書の種類を識別する識別子と他の端末の動作モードとを有するビーコン情報を含む信号を当該他の端末から受信するための受信手段と、

前記自端末の動作モードと前記他の端末の動作モードとが合致する場合に前記端末権限認証証明書テーブルに保持された端末権限認証証明書のうち前記受信手段により受信された信号に含まれる前記識別子に合致するものを提示して前記他の端末に対して自端末の認証を要求する認証要求手段と
を具備することを特徴とする端末。

【請求項 1 7】 前記端末権限認証証明書の種類を識別する識別子は、当該端末権限認証証明書を発行した端末の端末識別子であることを特徴とする請求項 1 6 記載の端末。

【請求項 1 8】 端末権限認証証明書発行端末の公開鍵証明書を保持する端末権限認証証明書発行端末リストテーブルと、

前記認証要求手段による認証要求に応答して前記他の端末が要求する第 2 の認

証要求を受信する認証要求受信手段と、

この認証要求受信手段が受信した前記第 2 の認証要求に含まれる第 2 の端末権限認証証明書を前記端末権限認証証明書発行端末リストテーブルに保持された公開鍵証明書に含まれる公開鍵によって検証する検証手段と、

前記検証に成功した場合において前記第 2 の端末権限認証証明書に含まれる可能動作モードによって前記他の端末の動作モードが許容されていなければ前記第 2 の認証要求は失敗したものとする動作モード確認手段と
をさらに具備することを特徴とする請求項 1 6 記載の端末。

【請求項 1 9】 前記端末権限認証証明書の種類を識別する識別子は、当該端末権限認証証明書を発行した端末の端末識別子であり、

前記端末権限認証証明書発行端末リストテーブルは、前記端末権限認証証明書を発行した端末の端末識別子と、前記端末権限認証証明書を発行した端末の公開鍵証明書と、前記端末権限認証証明書の前記端末権限認証証明書テーブルにおける格納位置とを関連付けて記憶すること
を特徴とする請求項 1 8 記載の端末。

【請求項 2 0】 前記他の端末との間で使用する管理ポリシーを保持するポリシーテーブルと、

前記動作モード確認手段によって第 2 の認証要求に失敗したものとされなかった場合には前記第 2 の端末権限認証証明書に含まれる管理ポリシーを前記ポリシーテーブルに設定する管理ポリシー設定手段と
をさらに具備することを特徴とする請求項 1 8 記載の端末。

【請求項 2 1】 自端末のアクセス権限を示す端末権限認証証明書を保持する端末権限認証証明書テーブルと、

自端末の動作モードを含む状態テーブルと、

前記端末権限認証証明書テーブルにおける端末権限認証証明書の種類を識別する識別子と前記自端末の動作モードとを有するビーコン情報を含む信号を他の端末に対して送信する送信手段と
を具備することを特徴とする端末。

【請求項 2 2】 前記端末権限認証証明書の種類を識別する識別子は、当該

端末権限認証証明書を発行した端末の端末識別子であることを特徴とする請求項 2 1 記載の端末。

【請求項 2 3】 自端末のアクセス権限を示す端末権限認証証明書を複数保持する端末権限認証証明書テーブルと、

自端末の動作モードを含む状態テーブルと、

前記端末権限認証証明書テーブルにおける複数の端末権限認証証明書から一つの端末権限認証証明書を選択するよう促す選択手段と、

この選択手段において選択された端末権限認証証明書の種類を識別する識別子と前記自端末の動作モードとを有するビーコン情報を含む信号を他の端末に対して送信する送信手段とを具備することを特徴とする端末。

【請求項 2 4】 前記端末権限認証証明書の種類を識別する識別子は、当該端末権限認証証明書を発行した端末の端末識別子であることを特徴とする請求項 2 3 記載の端末。

【請求項 2 5】 自端末のアクセス権限を示す端末権限認証証明書を保持する端末権限認証証明書テーブルと、自端末の動作モードを含む状態テーブルとを備える端末において、

端末権限認証証明書の種類を識別する識別子と他の端末の動作モードとを有するビーコン情報を含む信号を当該他の端末から受信する手順と、

前記自端末の動作モードと前記他の端末の動作モードとが合致する場合に前記端末権限認証証明書テーブルに保持された端末権限認証証明書のうち前記信号に含まれる前記識別子に合致するものを提示して前記他の端末に対して自端末の認証を要求する手順とを具備することを特徴とする処理方法。

【請求項 2 6】 自端末のアクセス権限を示す端末権限認証証明書を複数保持する端末権限認証証明書テーブルと、自端末の動作モードを含む状態テーブルとを備える端末において、

前記端末権限認証証明書テーブルにおける複数の端末権限認証証明書から一つの端末権限認証証明書を選択するよう促す手段と、

選択された端末権限認証証明書の種類を識別する識別子と前記自端末の動作モードとを有するビーコン情報を含む信号を他の端末に対して送信する手順とを具備することを特徴とする処理方法。

【請求項 2 7】 自端末のアクセス権限を示す端末権限認証証明書を保持する端末権限認証証明書テーブルと、自端末の動作モードを含む状態テーブルとを備える端末に、

端末権限認証証明書の種類を識別する識別子と他の端末の動作モードとを有するビーコン情報を含む信号を当該他の端末から受信する手順と、

前記自端末の動作モードと前記他の端末の動作モードとが合致する場合に前記端末権限認証証明書テーブルに保持された端末権限認証証明書のうち前記信号に含まれる前記識別子に合致するものを提示して前記他の端末に対して自端末の認証を要求する手順と
を実行させることを特徴とするプログラム。

【請求項 2 8】 自端末のアクセス権限を示す端末権限認証証明書を複数保持する端末権限認証証明書テーブルと、自端末の動作モードを含む状態テーブルとを備える端末に、

前記端末権限認証証明書テーブルにおける複数の端末権限認証証明書から一つの端末権限認証証明書を選択するよう促す手段と、

選択された端末権限認証証明書の種類を識別する識別子と前記自端末の動作モードとを有するビーコン情報を含む信号を他の端末に対して送信する手順とを実行させることを特徴とするプログラム。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、無線通信システムに関し、特に端末権限認証証明書を用いてネットワークへのアクセス権限を認証させる無線通信システム、当該システムにおける端末、および、これらにおける処理方法ならびに当該方法をコンピュータ（端末）に実行させるプログラムに関する。特に、本発明は、ネットワークを構成する全ての無線端末が管理情報（例えば、ビーコン等）を送信する無線ネットワーク

において有用である。

【0002】

【従来の技術】

無線通信システムにおいて各端末をネットワークに接続する際には、ネットワーク管理者が一意に定めた識別子（例えば、拡張サービスセット識別子（ESSID: Extended Service Set Identifier）等）をアクセスポイントに手動で設定しておき、そのアクセスポイントを利用する利用者が自身の無線端末に対してその識別子を設定することで、ネットワークと端末との対応を関係付けている。これにより、インフラストラクチャモードによる複数のネットワークが混在する環境においても、所望のアクセスポイントを一意に識別することができる。

【0003】

また、特定のアクセスポイントが存在しないインフラストラクチャモードにおいても、ネットワーク管理者が一意に定めた識別子をネットワーク管理者または利用者が手動で各端末に設定することにより、互いの端末が同じネットワークに属するか否かを識別することができる。

【0004】

このような無線通信システムにおける識別子の一例として、例えば、拡張サービスセット識別子（ESSID）とは異なる識別子を別個に定義して、それを工場出荷時に設定し、もしくは、任意に書き換えられるようにしておき、接続要求とともに送られてきた識別子と自己の識別子とが一致する場合に接続を許可し、一致しなければ接続を拒否するシステムが提案されている（例えば、特許文献1参照。）。

【0005】

【特許文献1】

特開 2002-198971号公報（図4）

【0006】

【発明が解決しようとする課題】

上述の従来技術では、ネットワーク毎に定められた識別子を各端末に手動で設

定するか、または、予め工場出荷時に設定しておく等の手順を必要としている。しかしながら、識別子の設定を手動で行うのは利用者にとって手間であり、また、誤入力を引き起こすおそれもある。また、予め設定しておいた場合でも、ネットワーク構造の変更等により識別子の設定に変更を要することもあり、利用者の負担は軽減されない。

【0 0 0 7】

また、識別子が一致する全ての端末に対して同じ条件でネットワークへのアクセスを認めてしまうと、無条件の公開を意図しないファイルへのアクセスも可能となり、セキュリティ上の問題が生じる。従って、ネットワークへの接続とは異なる観点による権限管理が必要となる。

【0 0 0 8】

一方、例えば属性証明書に代表されるような端末権限認証証明書を用いて権限管理を行うことが考えられるが、その場合、証明書発行者の公開鍵を用いた検証の手順を踏む必要があり、ビーコンの交換のように定期的に行われる動作において常に端末権限認証証明書を交換するのは現実的ではない。

【0 0 0 9】

そこで、本発明の目的は、無線通信システムのネットワークに接続しようとする端末において接続対象のネットワークを識別させ、または、接続対象のネットワークにおける権限を提示させることにある。

【0 0 1 0】

【課題を解決するための手段】

上記課題を解決するために本発明の請求項 1 記載の無線通信システムは、複数の端末により構成される無線通信システムであって、端末権限認証証明書の種類を識別する識別子を有するビーコン情報を含む信号を送信する第 1 の端末と、上記信号に応答して上記識別子に合致する種類の端末権限認証証明書を提示して上記第 1 の端末に対して認証を要求する第 2 の端末とを具備する。これにより、第 1 の端末からのビーコン情報を含む信号をトリガーとして、その信号に含まれる識別子に合致する種類の端末権限認証証明書を提示した認証要求を起動させるという作用をもたらす。

【0011】

また、本発明の請求項2記載の無線通信システムは、複数の端末により構成される無線通信システムであって、当該端末における動作モードを示すビーコン情報を含む信号を送信する第1の端末と、上記信号に応答して上記第1の端末における動作モードと自端末における動作モードとが一致している場合に、上記自端末における動作モードに関する権限を示す端末権限認証証明書を提示して上記第1の端末に対して認証を要求する第2の端末とを具備する。これにより、第1の端末からのビーコン情報を含む信号を受信した第2の端末に動作モードが合致していることを確認させるとともに、第1の端末において第2の端末の可能動作モードを確認させるという作用をもたらす。

【0012】

また、本発明の請求項3記載の端末は、自端末のアクセス権限を示す端末権限認証証明書を格納する端末権限認証証明書テーブルと、端末権限認証証明書の種類を識別する識別子を有するビーコン情報を含む信号を他の端末から受信するための受信手段と、上記端末権限認証証明書テーブルに保持された端末権限認証証明書のうち上記受信手段により受信された信号に含まれる上記識別子に合致するものを提示して上記他の端末に対して自端末の認証を要求する認証要求手段とを具備する。これにより、他の端末からのビーコン情報を含む信号をトリガーとして、その信号に含まれる識別子に合致する種類の端末権限認証証明書を提示した認証要求を起動させるという作用をもたらす。

【0013】

また、本発明の請求項4記載の端末は、請求項3記載の端末において、上記端末権限認証証明書の種類を識別する識別子が、当該端末権限認証証明書を発行した端末の端末識別子である。これにより、提示すべき端末権限認証証明書を端末権限認証証明書発行端末の端末識別子により識別させるという作用をもたらす。

【0014】

また、本発明の請求項5記載の端末は、請求項3記載の端末において、端末権限認証証明書発行端末の公開鍵証明書を保持する端末権限認証証明書発行端末リストテーブルと、上記認証要求手段による認証要求に応答して上記他の端末が要

求する第2の認証要求を受信する認証要求受信手段と、この認証要求受信手段が受信した上記第2の認証要求に含まれる第2の端末権限認証証明書を上記端末権限認証証明書発行端末リストテーブルに保持された公開鍵証明書に含まれる公開鍵によって検証する検証手段とをさらに具備する。これにより、ビーコン情報を含む信号の送信端末のアクセス権限を示す端末権限認証証明書を当該信号の受信端末に検証させるという作用をもたらす。

【0015】

また、本発明の請求項6記載の端末は、請求項5記載の端末において、上記端末権限認証証明書の種類を識別する識別子が、当該端末権限認証証明書を発行した端末の端末識別子であり、上記端末権限認証証明書発行端末リストテーブルが、上記端末権限認証証明書を発行した端末の端末識別子と、上記端末権限認証証明書を発行した端末の公開鍵証明書と、上記端末権限認証証明書の上記端末権限認証証明書テーブルにおける格納位置とを関連付けて記憶するものである。これにより、端末権限認証証明書の種類を識別する識別子と端末権限認証証明書とを関連付けさせるという作用をもたらす。

【0016】

また、本発明の請求項7記載の端末は、自端末のアクセス権限を示す端末権限認証証明書を保持する端末権限認証証明書テーブルと、この端末権限認証証明書テーブルにおける端末権限認証証明書の種類を識別する識別子を有するビーコン情報を含む信号を他の端末に対して送信する送信手段とを具備する。これにより、ビーコン情報を含む信号を受信した端末に対して認証要求の際に提示すべき端末権限認証証明書の種類を知らせるという作用をもたらす。

【0017】

また、本発明の請求項8記載の端末は、請求項7記載の端末において、上記端末権限認証証明書の種類を識別する識別子が、当該端末権限認証証明書を発行した端末の端末識別子である。これにより、提示すべき端末権限認証証明書を端末権限認証証明書発行端末の端末識別子により識別させるという作用をもたらす。

【0018】

また、本発明の請求項9記載の端末は、自端末のアクセス権限を示す端末権限

認証証明書を複数保持する端末権限認証証明書テーブルと、この端末権限認証証明書テーブルにおける複数の端末権限認証証明書から一つの端末権限認証証明書を選択するよう促す選択手段と、この選択手段において選択された端末権限認証証明書の種類を識別する識別子を有するビーコン情報を含む信号を他の端末に対して送信する送信手段とを具備する。これにより、複数の端末権限認証証明書から選択されたものを認証要求の際に提示すべき端末権限認証証明書の種類として知らせるという作用をもたらす。

【0019】

また、本発明の請求項10記載の端末は、請求項9記載の端末において、上記端末権限認証証明書の種類を識別する識別子が、当該端末権限認証証明書を発行した端末の端末識別子である。これにより、提示すべき端末権限認証証明書を端末権限認証証明書発行端末の端末識別子により識別させるという作用をもたらす。

【0020】

また、本発明の請求項11記載の端末は、自端末のアクセス権限を示す端末権限認証証明書を格納する端末権限認証証明書テーブルと、自端末の動作モードを含む状態テーブルと、他の端末の動作モードを有するビーコン情報を含む信号を当該他の端末から受信するための受信手段と、上記自端末の動作モードと上記他の端末の動作モードとが合致する場合に上記端末権限認証証明書テーブルに保持された端末権限認証証明書を提示して上記他の端末に対して自端末の認証を要求する認証要求手段とを具備する。これにより、動作モードの合致する相手端末に対して認証要求を行い、相手端末において自端末の可能動作モードを確認させるという作用をもたらす。

【0021】

また、本発明の請求項12記載の端末は、請求項11記載の端末において、端末権限認証証明書発行端末の公開鍵証明書を保持する端末権限認証証明書発行端末リストテーブルと、上記認証要求手段による認証要求に応答して上記他の端末が要求する第2の認証要求を受信する認証要求受信手段と、この認証要求受信手段が受信した上記第2の認証要求に含まれる第2の端末権限認証証明書を上記端

末権限認証証明書発行端末リストテーブルに保持された公開鍵証明書に含まれる公開鍵によって検証する検証手段と、上記検証に成功した場合において上記第2の端末権限認証証明書に含まれる可能動作モードによって上記他の端末の動作モードが許容されていなければ上記第2の認証要求は失敗したものとする動作モード確認手段とをさらに具備する。これにより、ビーコン情報に含まれた相手端末の動作モードが端末権限認証証明書によって許容されたものであるか否かを確認させるという作用をもたらす。

【0022】

また、本発明の請求項13記載の端末は、請求項12記載の端末において、上記端末権限認証証明書の種類を識別する識別子は、当該端末権限認証証明書を発行した端末の端末識別子であり、上記端末権限認証証明書発行端末リストテーブルは、上記端末権限認証証明書を発行した端末の端末識別子と、上記端末権限認証証明書を発行した端末の公開鍵証明書と、上記端末権限認証証明書の上記端末権限認証証明書テーブルにおける格納位置とを関連付けて記憶する。これにより、端末権限認証証明書の種類を識別する識別子と端末権限認証証明書とを関連付けさせるという作用をもたらす。

【0023】

また、本発明の請求項14記載の端末は、請求項12記載の端末において、上記他の端末との間で使用する管理ポリシーを保持するポリシーテーブルと、上記動作モード確認手段によって第2の認証要求に失敗したものとされなかった場合には上記第2の端末権限認証証明書に含まれる管理ポリシーを上記ポリシーテーブルに設定する管理ポリシー設定手段とをさらに具備する。これにより、相互認証の際に相手端末の端末権限認証証明書に含まれる管理ポリシーを当該相手端末との間の管理ポリシーとして設定せしめるという作用をもたらす。

【0024】

また、本発明の請求項15記載の端末は、自端末の動作モードを含む状態テーブルと、上記自端末の動作モードを有するビーコン情報を含む信号を他の端末に対して送信する送信手段とを具備する。これにより、当該信号を受信した端末において動作モードが合致することを確認せしめるという作用をもたらす。

【0025】

また、本発明の請求項16記載の端末は、自端末のアクセス権限を示す端末権限認証証明書を格納する端末権限認証証明書テーブルと、自端末の動作モードを含む状態テーブルと、端末権限認証証明書の種類を識別する識別子と他の端末の動作モードとを有するビーコン情報を含む信号を当該他の端末から受信するための受信手段と、上記自端末の動作モードと上記他の端末の動作モードとが合致する場合に上記端末権限認証証明書テーブルに保持された端末権限認証証明書のうち上記受信手段により受信された信号に含まれる上記識別子に合致するものを提示して上記他の端末に対して自端末の認証を要求する認証要求手段とを具備する。これにより、他の端末からのビーコン情報を含む信号をトリガーとして、その信号に含まれる識別子に合致する種類の端末権限認証証明書を提示した認証要求を動作モードの合致する相手端末に対して起動させるという作用をもたらす。

【0026】

また、本発明の請求項17記載の端末は、請求項16記載の端末において、上記端末権限認証証明書の種類を識別する識別子が、当該端末権限認証証明書を発行した端末の端末識別子である。これにより、提示すべき端末権限認証証明書を端末権限認証証明書発行端末の端末識別子により識別させるという作用をもたらす。

【0027】

また、本発明の請求項18記載の端末は、請求項16記載の端末において、端末権限認証証明書発行端末の公開鍵証明書を保持する端末権限認証証明書発行端末リストテーブルと、上記認証要求手段による認証要求に応答して上記他の端末が要求する第2の認証要求を受信する認証要求受信手段と、この認証要求受信手段が受信した上記第2の認証要求に含まれる第2の端末権限認証証明書を上記端末権限認証証明書発行端末リストテーブルに保持された公開鍵証明書に含まれる公開鍵によって検証する検証手段と、上記検証に成功した場合において上記第2の端末権限認証証明書に含まれる可能動作モードによって上記他の端末の動作モードが許容されていなければ上記第2の認証要求は失敗したものとする動作モード確認手段とをさらに具備する。これにより、ビーコン情報に含まれた相手端末

の動作モードが端末権限認証証明書によって許容されたものであるか否かを確認させるという作用をもたらす。

【0028】

また、本発明の請求項19記載の端末は、請求項18記載の端末において、上記端末権限認証証明書の種類を識別する識別子が、当該端末権限認証証明書を発行した端末の端末識別子であり、上記端末権限認証証明書発行端末リストテーブルは、上記端末権限認証証明書を発行した端末の端末識別子と、上記端末権限認証証明書を発行した端末の公開鍵証明書と、上記端末権限認証証明書の上記端末権限認証証明書テーブルにおける格納位置とを関連付けて記憶するものである。これにより、端末権限認証証明書の種類を識別する識別子と端末権限認証証明書とを関連付けさせるという作用をもたらす。

【0029】

また、本発明の請求項20記載の端末は、請求項18記載の端末において、上記他の端末との間で使用する管理ポリシーを保持するポリシーテーブルと、上記動作モード確認手段によって第2の認証要求に失敗したものとされなかった場合には上記第2の端末権限認証証明書に含まれる管理ポリシーを上記ポリシーテーブルに設定する管理ポリシー設定手段とをさらに具備する。これにより、相互認証の際に相手端末の端末権限認証証明書に含まれる管理ポリシーを当該相手端末との間の管理ポリシーとして設定せしめるという作用をもたらす。

【0030】

また、本発明の請求項21記載の端末は、自端末のアクセス権限を示す端末権限認証証明書を保持する端末権限認証証明書テーブルと、自端末の動作モードを含む状態テーブルと、上記端末権限認証証明書テーブルにおける端末権限認証証明書の種類を識別する識別子と上記自端末の動作モードとを有するビーコン情報を含む信号を他の端末に対して送信する送信手段とを具備する。これにより、ビーコン情報を含む信号を受信した端末に対して認証要求の際に提示すべき端末権限認証証明書の種類を知らせるとともに、動作モードが合致することを確認せしめるという作用をもたらす。

【0031】

また、本発明の請求項 2 2 記載の端末は、請求項 2 1 記載の端末において、上記端末権限認証証明書の種類を識別する識別子が、当該端末権限認証証明書を発行した端末の端末識別子である。これにより、提示すべき端末権限認証証明書を端末権限認証証明書発行端末の端末識別子により識別させるという作用をもたらす。

【0 0 3 2】

また、本発明の請求項 2 3 記載の端末は、自端末のアクセス権限を示す端末権限認証証明書を複数保持する端末権限認証証明書テーブルと、自端末の動作モードを含む状態テーブルと、上記端末権限認証証明書テーブルにおける複数の端末権限認証証明書から一つの端末権限認証証明書を選択するよう促す選択手段と、この選択手段において選択された端末権限認証証明書の種類を識別する識別子と上記自端末の動作モードとを有するビーコン情報を含む信号を他の端末に対して送信する送信手段とを具備する。これにより、複数の端末権限認証証明書から選択されたものを認証要求の際に提示すべき端末権限認証証明書の種類として知らせるという作用をもたらす。

【0 0 3 3】

また、本発明の請求項 2 4 記載の端末は、請求項 2 3 記載の端末において、上記端末権限認証証明書の種類を識別する識別子が、当該端末権限認証証明書を発行した端末の端末識別子である。これにより、提示すべき端末権限認証証明書を端末権限認証証明書発行端末の端末識別子により識別させるという作用をもたらす。

【0 0 3 4】

また、本発明の請求項 2 5 記載の処理方法は、自端末のアクセス権限を示す端末権限認証証明書を保持する端末権限認証証明書テーブルと、自端末の動作モードを含む状態テーブルとを備える端末において、端末権限認証証明書の種類を識別する識別子と他の端末の動作モードとを有するビーコン情報を含む信号を当該他の端末から受信する手順と、上記自端末の動作モードと上記他の端末の動作モードとが合致する場合に上記端末権限認証証明書テーブルに保持された端末権限認証証明書のうち上記信号に含まれる上記識別子に合致するものを提示して上記

他の端末に対して自端末の認証を要求する手順とを具備するものである。これにより、他の端末からのビーコン情報を含む信号をトリガーとして、その信号に含まれる識別子に合致する種類の端末権限認証証明書を提示した認証要求を動作モードの合致する相手端末に対して起動させるという作用をもたらす。

【0035】

また、本発明の請求項 26 記載の処理方法は、自端末のアクセス権限を示す端末権限認証証明書を複数保持する端末権限認証証明書テーブルと、自端末の動作モードを含む状態テーブルとを備える端末において、上記端末権限認証証明書テーブルにおける複数の端末権限認証証明書から一つの端末権限認証証明書を選択するよう促す手段と、選択された端末権限認証証明書の種類を識別する識別子と上記自端末の動作モードとを有するビーコン情報を含む信号を他の端末に対して送信する手順とを具備するものである。これにより、複数の端末権限認証証明書から選択されたものを認証要求の際に提示すべき端末権限認証証明書の種類として知らせるという作用をもたらす。

【0036】

また、本発明の請求項 27 記載のプログラムは、自端末のアクセス権限を示す端末権限認証証明書を保持する端末権限認証証明書テーブルと、自端末の動作モードを含む状態テーブルとを備える端末に、端末権限認証証明書の種類を識別する識別子と他の端末の動作モードとを有するビーコン情報を含む信号を当該他の端末から受信する手順と、上記自端末の動作モードと上記他の端末の動作モードとが合致する場合に上記端末権限認証証明書テーブルに保持された端末権限認証証明書のうち上記信号に含まれる上記識別子に合致するものを提示して上記他の端末に対して自端末の認証を要求する手順とを実行させるものである。これにより、他の端末からのビーコン情報を含む信号をトリガーとして、その信号に含まれる識別子に合致する種類の端末権限認証証明書を提示した認証要求を動作モードの合致する相手端末に対して起動させるという作用をもたらす。

【0037】

また、本発明の請求項 28 記載のプログラムは、自端末のアクセス権限を示す端末権限認証証明書を複数保持する端末権限認証証明書テーブルと、自端末の動

作モードを含む状態テーブルとを備える端末に、上記端末権限認証証明書テーブルにおける複数の端末権限認証証明書から一つの端末権限認証証明書を選択するよう促す手段と、選択された端末権限認証証明書の種類を識別する識別子と上記自端末の動作モードとを有するビーコン情報を含む信号を他の端末に対して送信する手順とを実行させるものである。これにより、複数の端末権限認証証明書から選択されたものを認証要求の際に提示すべき端末権限認証証明書の種類として知らせるという作用をもたらす。

【0038】

【発明の実施の形態】

次に本発明の実施の形態について図面を参照して詳細に説明する。

【0039】

図1は、本発明の実施の形態における無線通信システムにおいて使用される無線端末300の構成例を示す図である。無線端末300は、通信処理部320と、制御部330と、表示部340と、操作部350と、スピーカ360と、マイク370と、メモリ600とを備え、これらの間をバス380が接続する構成となっている。また、通信処理部320にはアンテナ310が接続されている。通信処理部320は、アンテナ310を介して受信した信号からネットワークインターフェース層（データリンク層）のフレームを構成する。また、通信処理部320は、ネットワークインターフェース層のフレームをアンテナ310を介して送信する。

【0040】

制御部330は、無線端末300全体を制御する。例えば、通信処理部320により構成されたフレームを参照して所定の処理を行う。表示部340は、所定の情報を表示するものであり、例えば、液晶ディスプレイ等が用いられ得る。操作部350は、無線端末300に対して外部から操作指示を行うためのものであり、例えば、キーボードやボタンスイッチ等が用いられ得る。スピーカ360は、音声を出力するものであり、無線端末300の利用者に対して注意を喚起したり他の端末と音声情報のやりとりを行うために用いられる。マイク370は、無線端末300に対して外部から音声入力を行うものであり、他の端末と音声情報

のやりとりを行ったり操作指示を行うために用いられる。

【0 0 4 1】

メモリ 6 0 0 は、属性証明書の発行端末に関する情報を保持する属性証明書発行端末リストテーブル 6 1 0 と、無線端末 3 0 0 自身のアクセス権限を示す属性証明書を格納する属性証明書テーブル 6 2 0 と、無線端末 3 0 0 自身の生成鍵に関する情報として公開鍵と秘密鍵と公開鍵証明書とを保持する生成鍵テーブル 6 5 0 と、無線端末 3 0 0 自身の動作状態を保持する状態テーブル 6 7 0 と、認証された各端末との間で使用する管理ポリシーを保持するポリシーテーブル 6 8 0 とを格納する。

【0 0 4 2】

図 2 は、本発明の実施の形態における属性証明書発行端末リストテーブル 6 1 0 の構成例である。この属性証明書発行端末リストテーブル 6 1 0 は、過去に属性証明書を発行した実績のある端末に関する情報を保持するものであり、属性証明書発行端末の端末識別子 6 1 1 のそれぞれに対応して、公開鍵証明書 6 1 2 および属性証明書インデックス 6 1 3 を保持している。

【0 0 4 3】

端末識別子 6 1 1 は、ネットワーク内において端末を一意に識別するものであればよく、例えば、イーサネット（登録商標）における MAC（Media Access Control）アドレス等を用いることができる。公開鍵証明書 6 1 2 は、対応する端末識別子 6 1 1 により識別される端末の公開鍵証明書である。公開鍵証明書とは、証明書所有者（サブジェクト）の本人性を証明するものであり、証明書所有者の公開鍵を含む。この公開鍵証明書は証明書発行者たる認証局（CA：Certificate Authority）によって署名される。また、属性証明書インデックス 6 1 3 は、属性証明書テーブル 6 2 0 における属性証明書の格納位置を示すものである。

【0 0 4 4】

図 3 は、属性証明書発行端末リストテーブル 6 1 0 に保持される公開鍵証明書 6 1 2 のフォーマット 7 1 0 を示す図である。この公開鍵証明書のフォーマット 7 1 0 は、大きく分けて、署名前証明書 7 1 1 と、署名アルゴリズム 7 1 8 と、

署名 7 1 9 とから構成される。署名前証明書 7 1 1 は、シリアル番号 7 1 2 と、発行者 7 1 4 と、有効期限 7 1 5 と、所有者 7 1 6 と、所有者 7 1 6 と、所有者公開鍵 7 1 7 とを含む。

【 0 0 4 5 】

シリアル番号 7 1 2 は、公開鍵証明書のシリアル番号であり、認証局によって採番される。発行者 7 1 4 は、公開鍵証明書の発行者たる認証局の名前である。この発行者 7 1 4 とシリアル番号 7 1 2 とにより公開鍵証明書は一意に識別される。有効期限 7 1 5 は、公開鍵証明書の有効期限である。所有者 7 1 6 は、公開鍵証明書の所有者の名前である。所有者公開鍵 7 1 7 は、所有者 7 1 6 の公開鍵である。

【 0 0 4 6 】

署名 7 1 9 は公開鍵証明書に対する認証局による署名であり、署名アルゴリズム 7 1 8 はこの署名 7 1 9 のために使用された署名アルゴリズムである。署名アルゴリズムは、メッセージダイジェストアルゴリズムと公開鍵暗号アルゴリズムの 2 つにより構成される。メッセージダイジェストアルゴリズムは、ハッシュ関数（要約関数）の一つであり、署名前証明書 7 1 1 のメッセージダイジェストを作成するためのアルゴリズムである。ここで、メッセージダイジェストとは、入力データ（署名前証明書 7 1 1）を固定長のビット列に圧縮したものであり、拇印や指紋（フィンガープリント）等とも呼ばれる。メッセージダイジェストアルゴリズムとしては、SHA-1（Secure Hash Algorithm 1）、MD2（Message Digest #2）、MD5（Message Digest #5）等が知られている。公開鍵暗号アルゴリズムは、メッセージダイジェストアルゴリズムにより得られたメッセージダイジェストを認証局の秘密鍵により暗号化するためのアルゴリズムである。この公開鍵暗号アルゴリズムとしては、素因数分解問題に基づく RSA や離散対数問題に基づく DSA 等が知られている。このように、署名前証明書 7 1 1 のメッセージダイジェストを認証局の秘密鍵により暗号化したものが署名 7 1 9 となる。

【 0 0 4 7 】

従って、この公開鍵証明書の署名 7 1 9 を認証局の公開鍵により復号すること

によってメッセージダイジェストが得られる。公開鍵証明書の利用者は、署名前証明書 711 のメッセージダイジェストを自身で作成し、それを認証局の公開鍵により復号されたメッセージダイジェストと比較することにより、署名前証明書 711 の内容が改ざんされていないことを検証できる。

【0048】

図 4 は、本発明の実施の形態における属性証明書テーブル 620 の構成例である。この属性証明書テーブル 620 に格納される属性証明書 622 は、無線端末 300 自身のアクセス権限を示す属性証明書であり、複数の属性証明書発行端末から発行を受けている場合には複数の属性証明書が格納される。この属性証明書テーブル 620 では、属性証明書 622 のそれぞれにインデックス 621 が付されている。このインデックス 621 は、属性証明書発行端末リストテーブル 610 の属性証明書インデックス 613 により指し示されるものである。本発明の実施の形態においては、属性証明書発行端末リストテーブル 610 の端末識別子 611 を無線通信システムにおけるネットワークのネットワーク識別子として扱い、認証の際にネットワーク識別子が一致することを確認した上で、属性証明書インデックス 613 により指し示される属性証明書 622 を用いて相互認証を行う。

【0049】

図 5 は、本発明の実施の形態における属性証明書発行端末リストテーブル 610 と属性証明書テーブル 620 との関係を示す図である。属性証明書発行端末リストテーブル 610 では、属性証明書発行端末毎にその端末識別子 611 と、公開鍵証明書 612 と、属性証明書インデックス 613 とを関連付けて記憶しており、属性証明書インデックス 613 はさらに属性証明書テーブル 620 における属性証明書 622 の格納位置（すなわち、インデックス 621）を保持している。

【0050】

本発明の実施の形態における無線通信システムにおいては、一つのネットワーク内に複数の属性証明書発行端末が存在することを許容するが、その場合でもネットワークに接続するためには何れか一つの属性証明書発行端末から属性証明書

の発行を受ければ十分である。例えば、図 5 における属性証明書発行端末リストテーブル 6 1 0 の第 1 行目の端末と第 3 行目の端末とが同じネットワークにおける属性証明書発行端末であったとして、第 1 行目の端末が発行した属性証明書を属性証明書テーブル 6 2 0 の第 1 行目に格納していたとする。その場合、属性証明書発行端末リストテーブル 6 1 0 の属性証明書インデックス 6 1 3 において、第 1 行目の端末および第 3 行目の端末はともに、属性証明書テーブル 6 2 0 の第 1 行目の属性証明書を指し示すように設定される。これにより、属性証明書発行端末リストテーブル 6 1 0 の第 1 行目の端末が発行した属性証明書を有する端末と第 3 行目の端末が発行した属性証明書を有する端末との間で相互認証することが可能となる。

【 0 0 5 1 】

従って、上の例で、属性証明書発行端末リストテーブル 6 1 0 の第 3 行目の端末の端末識別子をネットワーク識別子として表示した端末に対しては、属性証明書発行端末リストテーブル 6 1 0 の第 3 行目の属性証明書インデックス 6 1 3 から辿った属性証明書テーブル 6 2 0 の第 1 行目の属性証明書を提示して認証要求を行うことができる。そのとき、相手端末に対しては属性証明書発行端末リストテーブル 6 1 0 の第 1 行目の端末の端末識別子をネットワーク識別子として表示することにより、相手端末における属性証明書の検証が可能となる。

【 0 0 5 2 】

なお、属性証明書発行端末リストテーブル 6 1 0 には、接続中のネットワークにおいて新たな属性証明書発行端末が発生する度に追加されていく。無線端末 3 0 0 は、後述のように「現在使用中の属性証明書の属性証明書テーブル 6 2 0 における格納位置」を状態テーブル 6 7 0 に保持しており、新たに追加された属性証明書発行端末については属性証明書インデックス 6 1 3 に「現在使用中の属性証明書の属性証明書テーブル 6 2 0 における格納位置」を設定する。このように、一つのネットワーク内に複数の属性証明書発行端末が存在する場合、2 台目以降の属性証明書発行端末に対しては属性証明書インデックス 6 1 3 から既存の属性証明書を指し示すように設定することにより、複数の属性証明書発行端末の端末識別子をネットワーク識別子として束ねることができる。

【0053】

図6は、本発明の実施の形態における属性証明書テーブル620に保持される属性証明書のフォーマット720を示す図である。この属性証明書は、大きく分けて、属性証明情報721と、署名アルゴリズム728と、署名729とから構成される。属性証明情報721は、所有者公開鍵証明書識別子723と、発行者724と、シリアル番号722と、有効期限725と、属性情報726と、エクステンション727とを含む。

【0054】

所有者公開鍵証明書識別子723は、属性証明書の所有者の公開鍵証明書を識別するためのものである。具体的には、公開鍵証明書710（図3）の発行者714とシリアル番号712とにより識別する。発行者724は、属性証明書の発行者たる属性認証局（AA: Attribute certificate Authority）の名称である。シリアル番号722は、属性証明書のシリアル番号であり、属性証明書の発行者たる属性認証局によって採番される。このシリアル番号722と発行者724とにより属性証明書は一意に識別される。有効期限725は、属性証明書の有効期限である。

【0055】

属性情報726は、属性証明書の所有者の権限や資格等の属性情報を保持するものである。例えば、当該端末において利用可能な動作モードや当該端末との間で利用される管理ポリシーが規定される。

【0056】

ここで、動作モードとしては、例えば、ネットワークに接続する各端末に制限なくアクセスを認めるパブリックモードと、プライベートモードによりネットワークに接続する端末同士のアクセスしか認めないプライベートモードとがある。各端末は、パブリックモードとプライベートモードの何れかの動作モードで動作する。属性証明書に規定された可能動作モードが「プライベートモード可能」であれば、その端末はパブリックモードおよびプライベートモードの何れかを動作モードとして選択することができ、その動作モードを適宜切り換えることができる。一方、属性証明書に規定された可能動作モードが「プライベートモード不可

(パブリックモードのみ)」であれば、その端末はパブリックモードでしか動作できず、プライベートモードに切り換えることはできない。

【0057】

また、管理ポリシーとしては、例えば、相手端末との通信におけるフレーム転送ポリシーや、サービス品質 (QoS: Quality of Service) ポリシー等がある。

【0058】

フレーム転送ポリシーとしては、端末間でフレームを中継する際のホップ数の制限や、リンクのメディアが複数ある場合の特定メディアへの限定等が考えられる。ホップ数の制限としては、例えば、プライベートモードでは1ホップしかさせない等が考えられる。また、特定メディアへの限定としては、例えば、2.4GHz帯、2.5GHz帯、5GHz帯、ミリ波帯、UWB (ウルトラワイドバンド) 等のうち、高速に動作可能なUWBや5GHz帯を優先して使用させる等が考えられる。

【0059】

サービス品質ポリシーとしては、使用するアプリケーション毎に優先制御や帯域保証を変更する等が考えられる。これにより、例えば、ビデオストリームにおいて、画質を優先させるか、動きの滑らかさを優先させるか等を選択できるようになる。

【0060】

エクステンション727は、不正利用の防止や追加情報の記述に利用されるものである。本発明の実施の形態では、動作モードや管理ポリシー等を属性情報726に記述するものとして説明しているが、これらをこのエクステンション727に記述するようにしてもよい。

【0061】

署名729は属性証明書に対する属性認証局による署名であり、署名アルゴリズム728はこの署名729のために使用された署名アルゴリズムである。署名アルゴリズムの内容については、前述の公開鍵証明書の署名アルゴリズム718と同様であり、属性証明情報721のメッセージダイジェストを属性認証局の秘

密鍵により暗号化したものが署名 729 となる。

【0062】

従って、この属性証明書の署名 729 を属性認証局の公開鍵により復号することによってメッセージダイジェストが得られる。属性証明書の利用者は、属性証明情報 721 のメッセージダイジェストを自身で作成し、それを属性認証局の公開鍵により復号されたメッセージダイジェストと比較することにより、属性証明情報 721 の内容が改ざんされていないことを検証できる。

【0063】

なお、本発明の実施の形態では、端末権限認証証明書の一例として属性証明書について説明するが、例えば、XML 言語等により端末権限を記述しておき、権限を有する機関がそれに署名を付することにより作成されたようなものであっても本発明における端末権限認証証明書として機能し得る。

【0064】

図 7 は、本発明の実施の形態における状態テーブル 670 の構成例である。状態テーブル 670 は、無線端末 300 自身の動作状態を保持するものであり、例えば、使用属性証明書インデックス 671、稼動動作モード 672、および、可能動作モード 673 等を保持する。

【0065】

使用属性証明書インデックス 671 は、現在使用中の属性証明書の属性証明書テーブル 620 における格納位置を保持する。ここにいう格納位置とは、具体的には、属性証明書テーブル 620 のインデックス 621 を意味する。また、現在使用中の属性証明書とはネットワークに接続するために使用している属性証明書であり、その属性証明書を発行した端末の端末識別子はネットワーク識別子として後述のように自己の存在を示すビーコン中に提示される。また、ネットワーク内の 2 台目以降の属性証明書発行端末を属性証明書発行端末リストテーブル 610 に登録する際には、使用属性証明書インデックス 671 の内容を属性証明書インデックス 613 に設定する。

【0066】

稼動動作モード 672 は、無線端末 300 自身において稼動中の動作モードを

示すものである。一方、可能動作モード673は、現在使用中の属性証明書によって許可されている動作モードを示すものである。可能動作モード673が「プライベートモード可能」であれば、パブリックモードおよびプライベートモードの何れかを稼動動作モード672として設定することができる。一方、可能動作モード673が「プライベートモード不可」であれば、稼動動作モード672としてパブリックモードしか設定できず、プライベートモードに設定することはできない。

【0067】

図8は、本発明の実施の形態におけるポリシーテーブル680の構成例である。このポリシーテーブル680は、認証された端末との間で上述のような各種の管理ポリシーを定めるものであり、相手端末の端末識別子681毎に管理ポリシー682を保持している。このポリシーテーブル680に対する設定は、属性証明書による相互認証の際に行われ、認証要求メッセージに含まれる相手端末の属性証明書の内容に従って設定される。例えば、ある端末Xの管理ポリシーとして、他の端末へのフレームを中継しないという管理ポリシーが端末Xの属性証明書に規定されている場合、端末Xと相互認証する端末はそのポリシーテーブル680において、端末Xの端末識別子681に対応する管理ポリシー682に端末Xの管理ポリシーを設定する。

【0068】

図9は、本発明の実施の形態における通信で使用されるフレーム構成を示す図である。フレーム800は、ヘッダ部801と、ペイロード部802とから構成される。また、ヘッダ部801は、始点端末識別子803と、終点端末識別子804と、送信端末識別子805と、受信端末識別子806と、フレーム種別807とを含む。また、ペイロード部802にはフレームの種別に応じたデータが格納される。

【0069】

始点端末識別子803は、このフレームを最初に発信した端末の端末識別子である。なお、端末識別子は、前述のようにネットワーク内において端末を一意に識別するものであればよく、例えば、イーサネット（登録商標）におけるMAC

アドレス等を用いることができる。終点端末識別子 8 0 4 は、このフレームの最終宛先の端末の端末識別子である。

【0 0 7 0】

送信端末識別子 8 0 5 および受信端末識別子 8 0 6 は、フレームを中継する際に用いられる。無線アドホック通信システムにおいては、ネットワーク内の全ての端末が直接通信できるとは限らず、電波の届かない端末へフレームを送信したい場合には他の端末を介してマルチホップにより通信経路を確立しなければならない。この場合にフレームの送受信を行う端末間で使用されるのが送信端末識別子 8 0 5 および受信端末識別子 8 0 6 である。フレーム種別 8 1 7 は、フレームの種別を示すものである。

【0 0 7 1】

次に本発明の実施の形態における無線通信システムの動作について図面を参照して説明する。

【0 0 7 2】

図 1 0 は、本発明の実施の形態における端末間の相互認証手順の一例を示す図である。ここで、端末 A (1 0 0) は既にネットワークに参入している無線端末であり、端末 B (2 0 0) は新たにネットワークに参入しようとしている無線端末である。

【0 0 7 3】

この相互認証手順では、端末 A が端末 B からのビーコンを受信することをきっかけとして処理が開始する。基地局を有する無線通信システムでは、基地局がビーコンを送信し、他の子局がそのビーコンを受信するように構成される。また、基地局を有さない無線アドホック通信システムでは、各端末が他の端末に自己の存在を知らせるべく、ビーコンを出し合うように構成される。なお、本発明の実施の形態において、ビーコンは、標識信号としてのビーコン情報のみを含む信号だけではなく、ビーコン情報に何らかのデータ情報が付加された信号をも含むものとする。

【0 0 7 4】

ビーコンの構成は、図 1 1 のフレーム構成による。ビーコンフレーム 8 1 0 は

、図 9 で説明したフレーム構成に準ずるものであり、ヘッダ部 8 1 1 とペイロード部 8 1 2 とに分けられる。ヘッダ部 8 1 1 における始点端末識別子 8 1 3、終点端末識別子 8 1 4、送信端末識別子 8 1 5、および、受信端末識別子 8 1 6 は、図 9 の構成と同様である。フレーム種別 8 1 7 は、当該フレームがビーコンフレームであることを示す。また、動作モード 8 1 8 には、ビーコン送信端末である端末 B の動作モードとして、状態テーブル 6 7 0 における稼動動作モード 6 7 2 が提示される。

【 0 0 7 5 】

ネットワーク識別子 8 1 9 には、ネットワーク接続のために使用する属性証明書の種類として、例えば、その属性証明書の発行端末の端末識別子が提示される。なお、この属性証明書の種類の識別子のフィールドに有効な端末識別子が保持されていない場合（例えば、全てゼロの場合）には、そのビーコン送信端末（端末 B）は属性証明書を有していないことになる。

【 0 0 7 6 】

無線端末 3 0 0 は、属性証明書テーブル 6 2 0 に複数の属性証明書を保有している場合、何れの属性証明書を使用してビーコンを送信するかを選択を利用者に促す。そのために、表示部 3 4 0、操作部 3 5 0、スピーカ 3 6 0、および、マイク 3 7 0 等が使用され得る。

【 0 0 7 7 】

このようなフレーム構成を有するビーコン 2 0 1 1 を端末 B が送信（2 0 1）すると、そのビーコン 2 0 1 1 は端末 A によって受信（1 0 1）される。端末 A は、端末 B からビーコンを受信（1 0 1）すると、ビーコンに提示された動作モード 8 1 8 と自端末の稼動動作モード 6 7 2 とが合致しているか否かを確認する（1 0 2）。これにより、合致する動作モードで動作する端末同士のみが互いにアクセスできるように制限することができる。

【 0 0 7 8 】

次に端末 A は、ビーコンに提示されたネットワーク識別子 8 1 9 に合致する端末識別子を属性証明書発行端末リストテーブル 6 1 0 の端末識別子 6 1 1 から検索し、その端末識別子 6 1 1 に対応する属性証明書インデックス 6 1 3 によって

属性証明書テーブル 6 2 0 を索引して、属性証明書 6 2 2 を選択する (1 0 3)

。

【0 0 7 9】

このようにして選択した属性証明書を提示して、端末 A は端末 B に対して認証要求メッセージ 1 1 1 2 を送信 (1 1 1) する。この認証要求メッセージ 1 1 1 2 のフレーム構成は、図 9 で説明したフレーム構成に準ずるものである。フレーム種別 8 0 7 は、当該フレームが認証要求フレームであることを示す。また、ペイロード部 8 1 2 には、データとして、端末 A の公開鍵証明書および属性証明書が含まれる。公開鍵証明書は端末 A の本人性を証明するためのものであり、属性証明書は端末 A の権限を証明するためのものである。

【0 0 8 0】

端末 B は、端末 A から認証要求メッセージ 1 1 1 2 を受けると、認証要求メッセージ 1 1 1 2 に含まれる属性証明書により端末 A を認証 (2 1 1) する。具体的には、属性証明書発行端末リストテーブル 6 1 0 の公開鍵証明書 6 1 2 (図 2) から属性認証局の公開鍵を抽出して、この公開鍵によって認証要求メッセージ 1 1 1 2 に含まれる属性証明書の署名 7 2 9 (図 6) を復号することにより署名時のメッセージダイジェストを得る。そして、属性証明書の属性証明情報 7 2 1 (図 6) のメッセージダイジェストを新たに生成する。この新たに生成されたメッセージダイジェストが署名時のメッセージダイジェストと一致していることを確認する。もしこれらが一致しないとすれば、属性証明書は署名後に改ざんされた可能性があり、属性証明書の検証は失敗となる。両者が一致している場合には、さらに認証要求メッセージ 1 1 1 2 に含まれる属性証明書の所有者公開鍵証明書識別子 7 2 3 (図 6) が、認証要求メッセージ 1 1 1 2 に含まれる公開鍵証明書の発行者 7 1 4 およびシリアル番号 7 1 2 (図 3) に一致することを確認する。これが一致すれば、公開鍵証明書の所有者である端末 A は属性証明書の所有者であることが確認できる。もしこれらが一致しないとすれば、属性証明書の所有者は端末 A ではなく、端末 A の認証は失敗となる。

【0 0 8 1】

端末 A の認証 (2 1 1) に成功すると、端末 B は、端末 A からの認証要求メッ

セージ 1 1 1 2 に含まれる属性証明書 of 属性情報 7 2 6 に規定される可能動作モードが端末 B における状態テーブル 6 7 0 の稼動動作モード 6 7 2 に合致しているか否かを確認 (2 1 2) する。これにより、例えば、プライベートモードにより動作する端末がビーコンを送信した際に、可能動作モードが「プライベートモード不可」である悪意のある端末から認証要求メッセージを受けた場合、その認証要求メッセージに含まれる属性証明書 of 属性情報 7 2 6 に規定される可能動作モードが「プライベートモード不可」となっているので、ビーコン送信端末はその認証要求を退けることができる。

【0082】

動作モードが合致していることを確認 (2 1 2) すると、端末 B は、認証要求メッセージ 1 1 1 2 に含まれる属性証明書 of 属性情報 7 2 6 に規定される管理ポリシーを端末 B におけるポリシーテーブル 6 8 0 の管理ポリシー 6 8 2 に設定 (2 1 3) する。そして、端末 B は、端末 A の認証に成功したことを通信する認証成功メッセージ 2 2 1 1 を端末 A に送信 (2 2 1) する。この認証成功メッセージ 2 2 1 1 のフレーム構成は図 9 で説明したフレーム構成に準ずるものである。フレーム種別 8 0 7 は、当該フレームが認証成功フレームであることを示す。また、ヘッダ部 8 0 1 には、さらにその理由の種別を示す情報が含まれる。一方、認証に失敗した場合の認証失敗フレームも、認証成功フレームと同様のフレーム構成を備える。

【0083】

次に端末 B は端末 A に対して認証要求メッセージ 2 3 1 1 を送信 (2 3 1) する。この認証要求メッセージ 2 3 1 1 のフレーム構成は、上述の認証要求メッセージ 1 1 1 2 と同様である。ペイロード部 8 1 2 には、データとして、端末 B の公開鍵証明書および属性証明書が含まれる。

【0084】

端末 A は、端末 B から認証要求メッセージ 2 3 1 1 を受けると、認証要求メッセージ 2 3 1 1 に含まれる属性証明書により端末 B を認証 (1 3 1) する。この認証の内容は既に説明した通りであり、属性証明書の検証、および、属性証明書の所有者の確認等が行われる。

【0085】

端末Bの認証(131)に成功すると、端末Aは、端末Bからの認証要求メッセージ2311に含まれる属性証明書の属性情報726に規定される可能動作モードが端末Aにおける状態テーブル670の稼動動作モード672に合致しているか否かを確認(132)する。これにより、例えば、可能動作モードが「プライベートモード不可」である悪意のある端末が「プライベートモード」によるビーコンを送信して、さらに認証要求を行ってきた場合に、その認証要求メッセージに含まれる属性証明書の属性情報726に規定される可能動作モードが「プライベートモード不可」となっているので、ビーコン受信端末はその認証要求を退けることができる。

【0086】

動作モードが合致していることを確認(132)すると、端末Aは、認証要求メッセージ2311に含まれる属性証明書の属性情報726に規定される管理ポリシーを端末Aにおけるポリシーテーブル680の管理ポリシー682に設定(133)する。そして、端末Aは、端末Bの認証に成功したことを通信する認証成功メッセージ1412を端末Bに送信(141)する。この認証成功メッセージ1412のフレーム構成は、上述の認証成功メッセージ2211と同様である。この認証成功メッセージ1412は、端末Bにより受信されて確認(241)される。

【0087】

このようにして、端末Aおよび端末Bにおいて互いの端末の認証に成功すると相互認証は完了する。

【0088】

次に本発明の実施の形態の無線通信システムの各端末における処理について図面を参照して説明する。

【0089】

図12は、図10の端末Aにおける相互認証処理の流れを示す図である。まず、端末Bからのビーコンを受信すると(ステップS911)、端末Aはビーコンに提示された動作モード818と自端末の稼動動作モード672とが合致してい

るか否かを確認する（ステップ S 9 1 2）。もし、両者が合致しないようであれば、認証要求を行わずに処理を終了する。

【 0 0 9 0 】

ステップ S 9 1 2 においてビーコンに提示された動作モード 8 1 8 と自端末の稼動動作モード 6 7 2 とが合致していた場合、端末 A はビーコンに提示されたネットワーク識別子 8 1 9 に合致する端末識別子を属性証明書発行端末リストテーブル 6 1 0 の端末識別子 6 1 1 から検索する（ステップ S 9 1 3）。もし、両者が合致しないようであれば、認証要求を行わずに処理を終了する。

【 0 0 9 1 】

ステップ S 9 1 3 においてビーコンに提示されたネットワーク識別子 8 1 9 に合致する端末識別子 6 1 1 が存在すれば、その端末識別子 6 1 1 に対応する属性証明書インデックス 6 1 3 によって指し示される属性証明書テーブル 6 2 0 の属性証明書 6 2 2 を提示した認証要求メッセージを端末 B に送信する（ステップ S 9 1 4）。この認証要求に対して、端末 B において認証に失敗した場合には、それ以上の処理は行わずに終了する（ステップ S 9 1 5）。

【 0 0 9 2 】

端末 B において認証に成功し（ステップ S 9 1 5）、さらに端末 B からの認証要求メッセージを受けると（ステップ S 9 1 6）、端末 A は端末 B の認証を行う（ステップ S 9 1 7）。もし、属性証明書を検証できない等の理由により端末 B を認証できない場合には（ステップ S 9 1 8）、端末 A は端末 B に認証失敗メッセージを送信する（ステップ S 9 2 3）。

【 0 0 9 3 】

ステップ S 9 1 8 において端末 B を認証できた場合、端末 A は端末 B からの認証要求メッセージに含まれる属性証明書の属性情報 7 2 6 に規定される可能動作モードが端末 A における状態テーブル 6 7 0 の稼動動作モード 6 7 2 に合致しているか否かを確認する（ステップ S 9 1 9）。もし、両動作モードが合致しない場合には、端末 A は端末 B に認証失敗メッセージを送信する（ステップ S 9 2 3）。

【 0 0 9 4 】

ステップ S 9 1 9 において両動作モードが合致した場合、端末 A は、認証要求メッセージに含まれる属性証明書の属性情報 7 2 6 に規定される管理ポリシーを端末 A におけるポリシーテーブル 6 8 0 の管理ポリシー 6 8 2 に設定する（ステップ S 9 2 1）。そして、端末 A は端末 B に認証成功メッセージを送信する（ステップ S 9 2 2）。

【0 0 9 5】

図 1 3 は、図 1 0 の端末 B における相互認証処理の流れを示す図である。まず、端末 B は、ネットワークに接続するための属性証明書に基づき動作モード 8 1 8 およびネットワーク識別子 8 1 9 を提示して、ビーコンを送信する（ステップ S 9 3 1）。そして、このビーコンに応答して端末 A から認証要求メッセージを受信すると（ステップ S 9 3 2）、端末 B は端末 A の認証を行う（ステップ S 9 3 3）。もし、属性証明書を検証できない等の理由により端末 A を認証できない場合には（ステップ S 9 3 4）、端末 B は端末 A に認証失敗メッセージを送信する（ステップ S 9 4 1）。

【0 0 9 6】

ステップ S 9 3 4 において端末 A を認証できた場合、端末 B は端末 A からの認証要求メッセージに含まれる属性証明書の属性情報 7 2 6 に規定される可能動作モードが端末 B における状態テーブル 6 7 0 の稼動動作モード 6 7 2 に合致しているか否かを確認する（ステップ S 9 3 5）。もし、両動作モードが合致しない場合には、端末 B は端末 A に認証失敗メッセージを送信する（ステップ S 9 4 1）。

【0 0 9 7】

ステップ S 9 3 5 において両動作モードが合致した場合、端末 B は、認証要求メッセージに含まれる属性証明書の属性情報 7 2 6 に規定される管理ポリシーを端末 B におけるポリシーテーブル 6 8 0 の管理ポリシー 6 8 2 に設定する（ステップ S 9 3 6）。そして、端末 B は端末 A に認証成功メッセージを送信する（ステップ S 9 3 7）。また、続いて端末 B は端末 A に認証要求メッセージを送信する（ステップ S 9 3 8）。その後、その認証要求メッセージに対する認証応答メッセージを受信する（ステップ S 9 3 9）。

【0098】

このように、本発明の実施の形態によれば、属性証明書発行端末の端末識別子をネットワーク識別子 819 としてビーコン内に提示させることにより、ネットワークと属性証明書との関連付けを行なうことができる。また、動作モード 818 をビーコン内に提示させることにより、ネットワークに接続する際にプライベートモードとして接続するのかパブリックモードとして接続するのかを即座に判断することができる。

【0099】

なお、本発明の実施の形態では、各端末が自律的に無線通信システムを構成する例について説明したが、何れかの端末が基地局として動作するような無線通信システムであっても構わない。

【0100】

また、ここでは本発明の実施の形態を例示したものであり、本発明はこれに限られず、本発明の要旨を逸脱しない範囲において種々の変形を施すことができる。

【0101】

また、ここで説明した処理手順はこれら一連の手順を有する方法として捉えてもよく、これら一連の手順をコンピュータ（端末）に実行させるためのプログラム乃至そのプログラムを記憶する記録媒体として捉えてもよい。

【0102】**【発明の効果】**

以上の説明で明らかなように、本発明によると、無線通信システムのネットワークに接続しようとする端末において接続対象のネットワークを識別させ、または、接続対象のネットワークにおける権限を提示させることができるという効果が得られる。

【図面の簡単な説明】**【図1】**

本発明の実施の形態における無線通信システムにおいて使用される無線端末 300 の構成例を示す図である。

【図 2】

本発明の実施の形態における属性証明書発行端末リストテーブル 6 1 0 の構成例である。

【図 3】

本発明の実施の形態における属性証明書発行端末リストテーブル 6 1 0 に保持される公開鍵証明書 6 1 2 のフォーマット 7 1 0 を示す図である。

【図 4】

本発明の実施の形態における属性証明書テーブル 6 2 0 の構成例である。

【図 5】

本発明の実施の形態における属性証明書発行端末リストテーブル 6 1 0 と属性証明書テーブル 6 2 0 との関係を示す図である。

【図 6】

本発明の実施の形態における属性証明書テーブル 6 2 0 に保持される属性証明書のフォーマット 7 2 0 を示す図である。

【図 7】

本発明の実施の形態における状態テーブル 6 7 0 の構成例である。

【図 8】

本発明の実施の形態におけるポリシーテーブル 6 8 0 の構成例である。

【図 9】

本発明の実施の形態における通信で使用されるフレーム構成を示す図である。

【図 1 0】

本発明の実施の形態における端末間の相互認証手順の一例を示す図である。

【図 1 1】

本発明の実施の形態におけるビーコンフレームのフレーム構成を示す図である。

【図 1 2】

本発明の実施の形態におけるビーコン受信端末における相互認証処理の流れを示す図である。

【図 1 3】

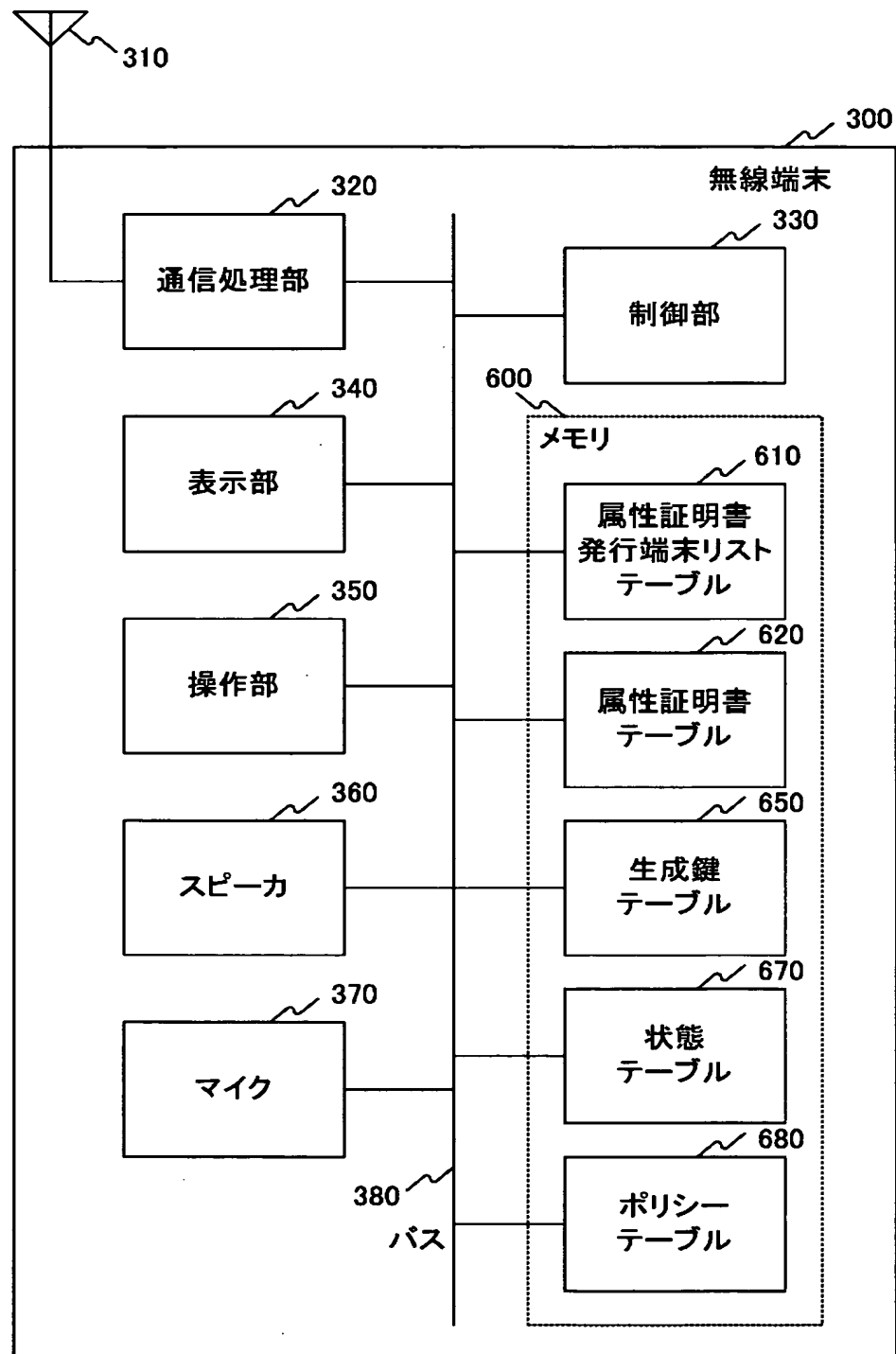
本発明の実施の形態におけるビーコン送信端末における相互認証処理の流れを示す図である。

【符号の説明】

- 1 0 0 端末 A (無線端末)
- 2 0 0 端末 B (無線端末)
- 3 0 0 無線端末
- 3 1 0 アンテナ
- 3 2 0 通信処理部
- 3 3 0 制御部
- 3 4 0 表示部
- 3 5 0 操作部
- 3 6 0 スピーカ
- 3 7 0 マイク
- 3 8 0 バス
- 6 0 0 メモリ
- 6 1 0 属性証明書発行端末リストテーブル
- 6 2 0 属性証明書テーブル
- 6 5 0 生成鍵テーブル
- 6 7 0 状態テーブル
- 6 8 0 ポリシーテーブル
- 7 1 0 公開鍵証明書
- 7 2 0 属性証明書
- 8 0 0 フレーム
- 8 1 0 ビーコンフレーム

【書類名】 図面

【図 1】

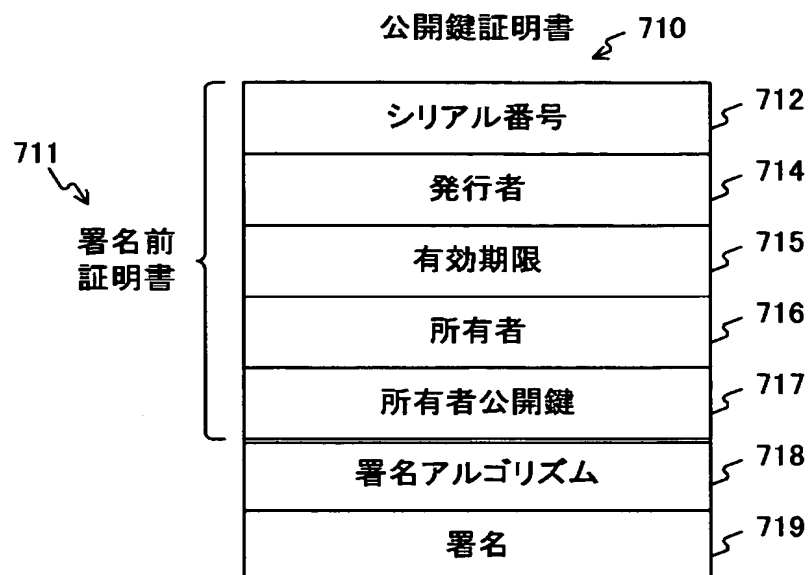


【図 2】

属性証明書発行端末リストテーブル 610

611	612	613
端末識別子 #1	公開鍵証明書 #1	属性証明書 インデックス #1
端末識別子 #2	公開鍵証明書 #2	属性証明書 インデックス #2
⋮	⋮	⋮

【図 3】

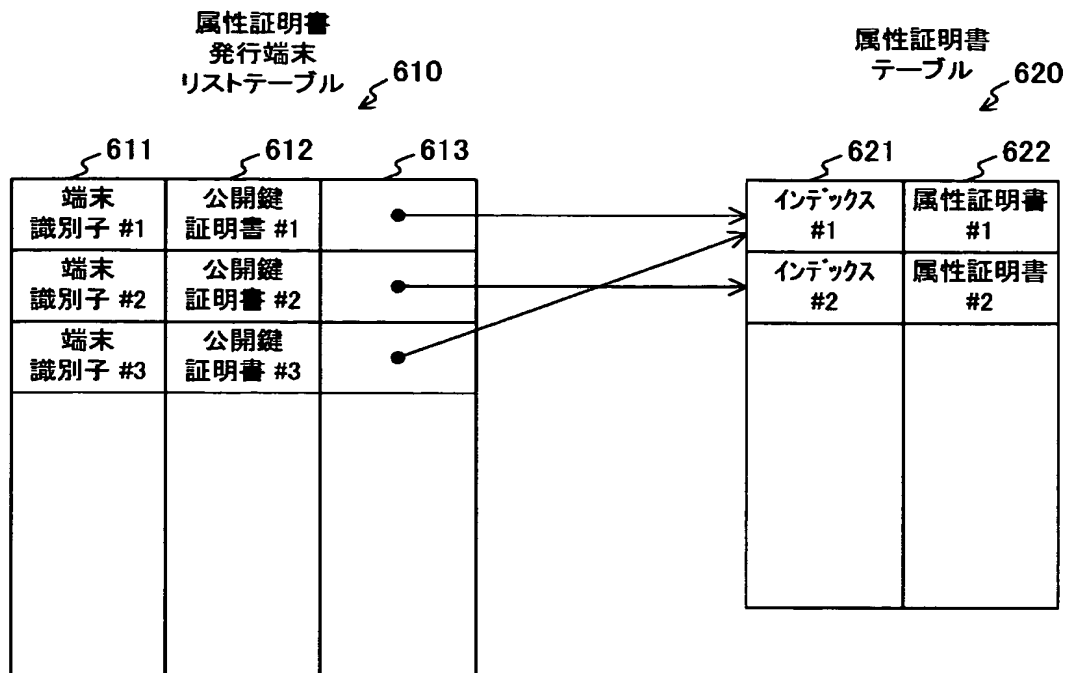


【図 4】

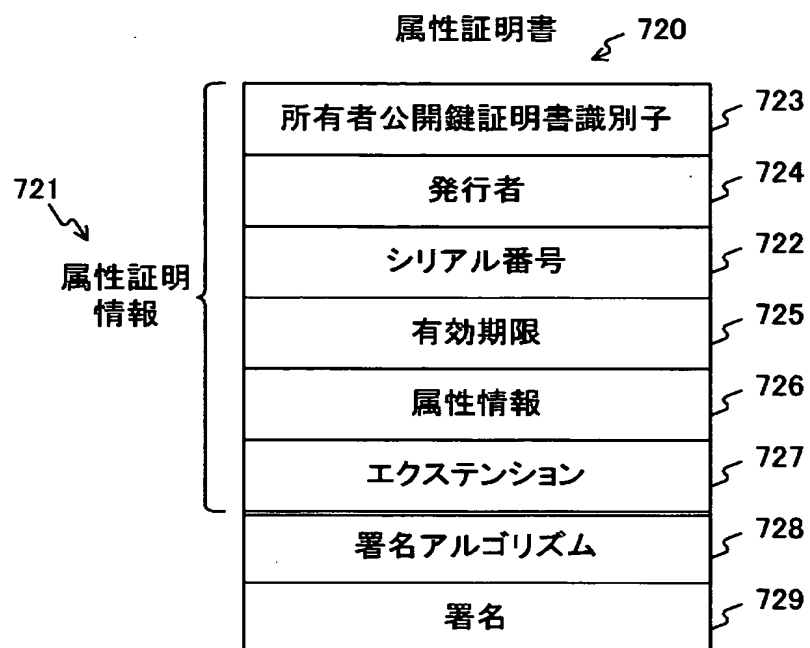
属性証明書テーブル 620

621	622
インデックス #1	属性証明書 #1
インデックス #2	属性証明書 #2
⋮	⋮

【図 5】



【図 6】



【図 7】

状態テーブル 670

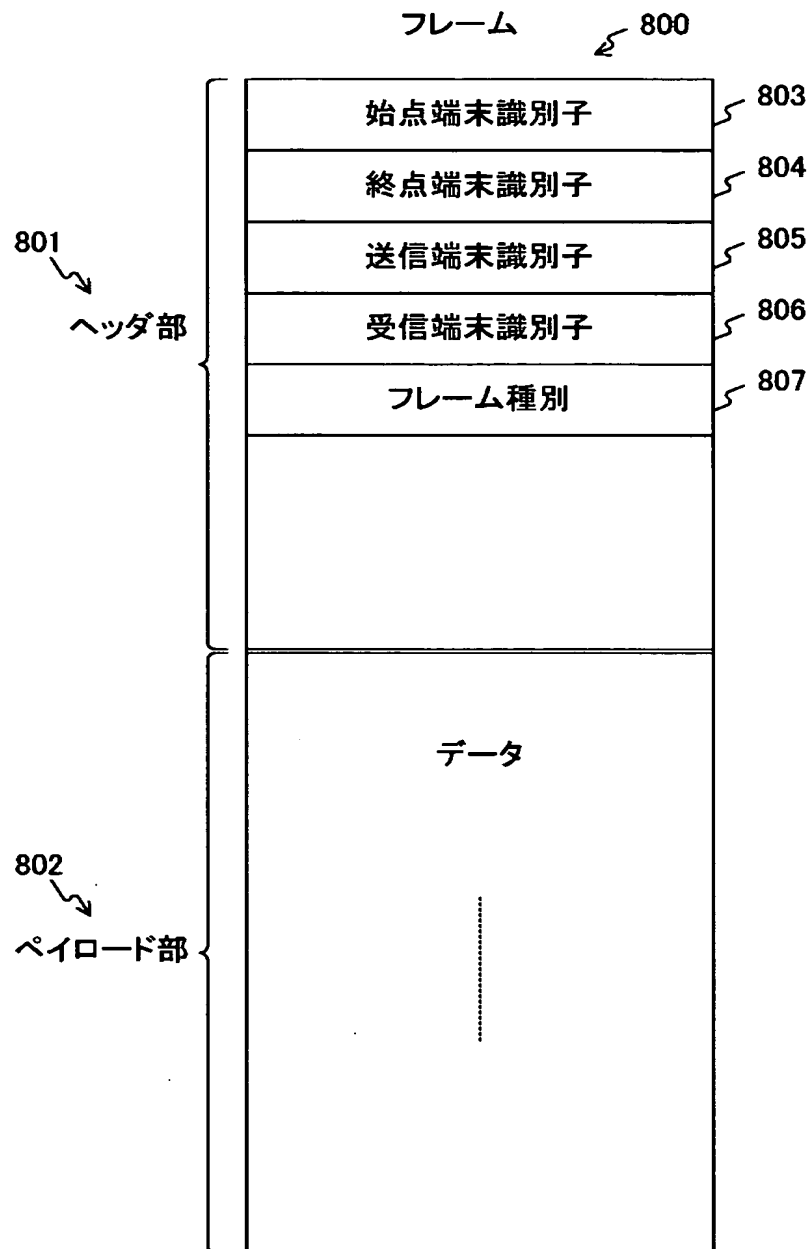
使用属性証明書インデックス	671
稼働動作モード	672
可能動作モード	673

【図 8】

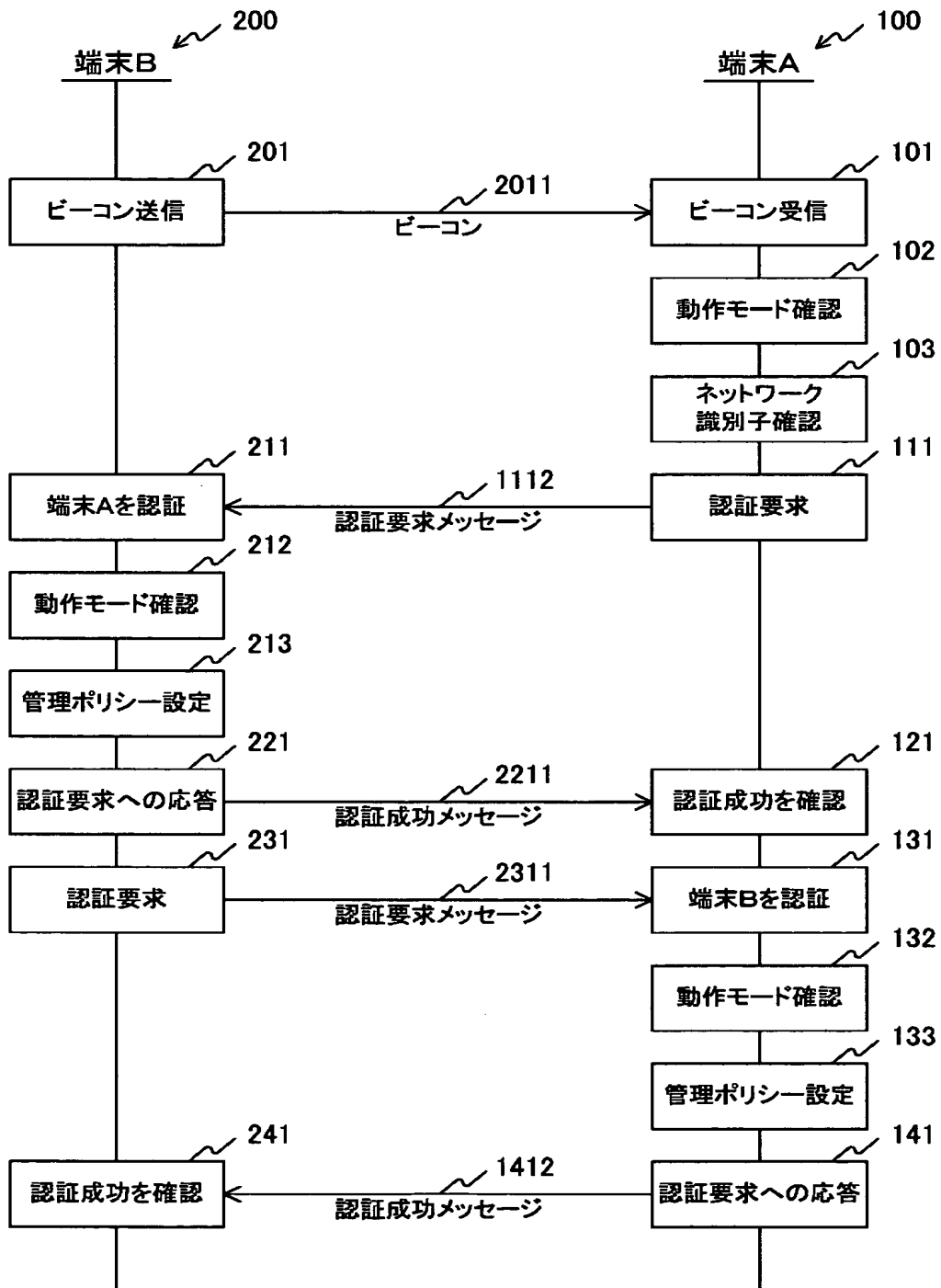
ポリシーテーブル 680

681	682
端末識別子 #1	管理ポリシー #1
端末識別子 #2	管理ポリシー #2
⋮	⋮

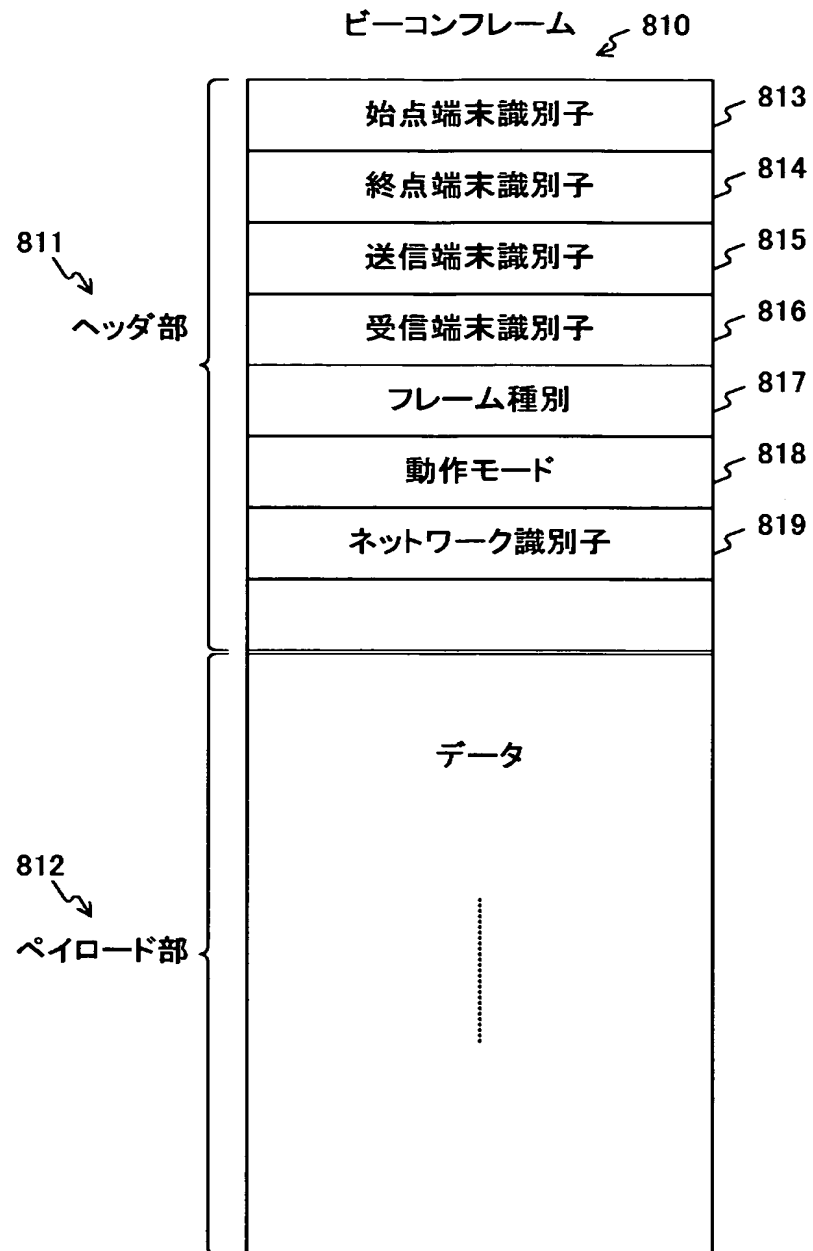
【図 9】



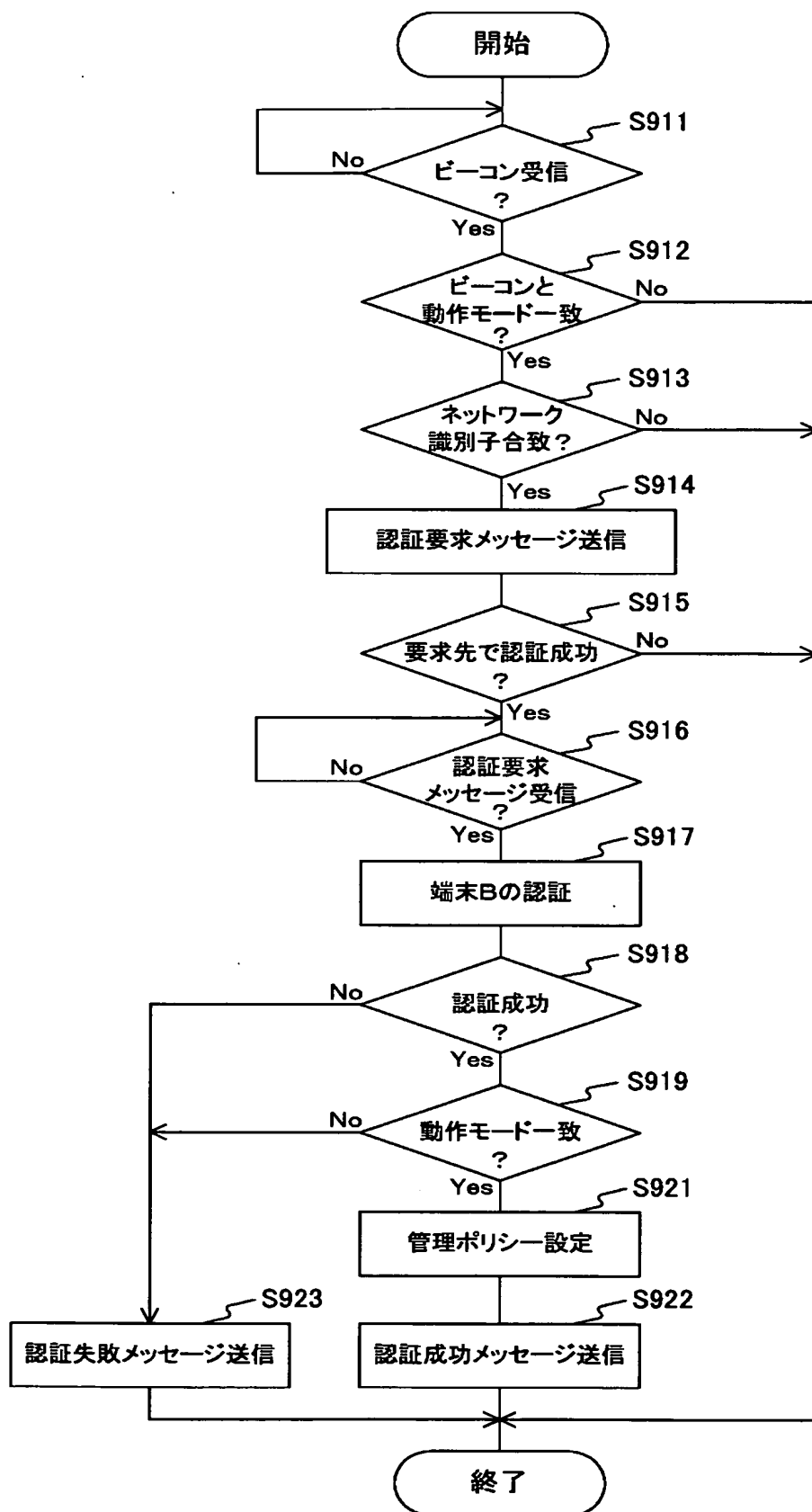
【図10】



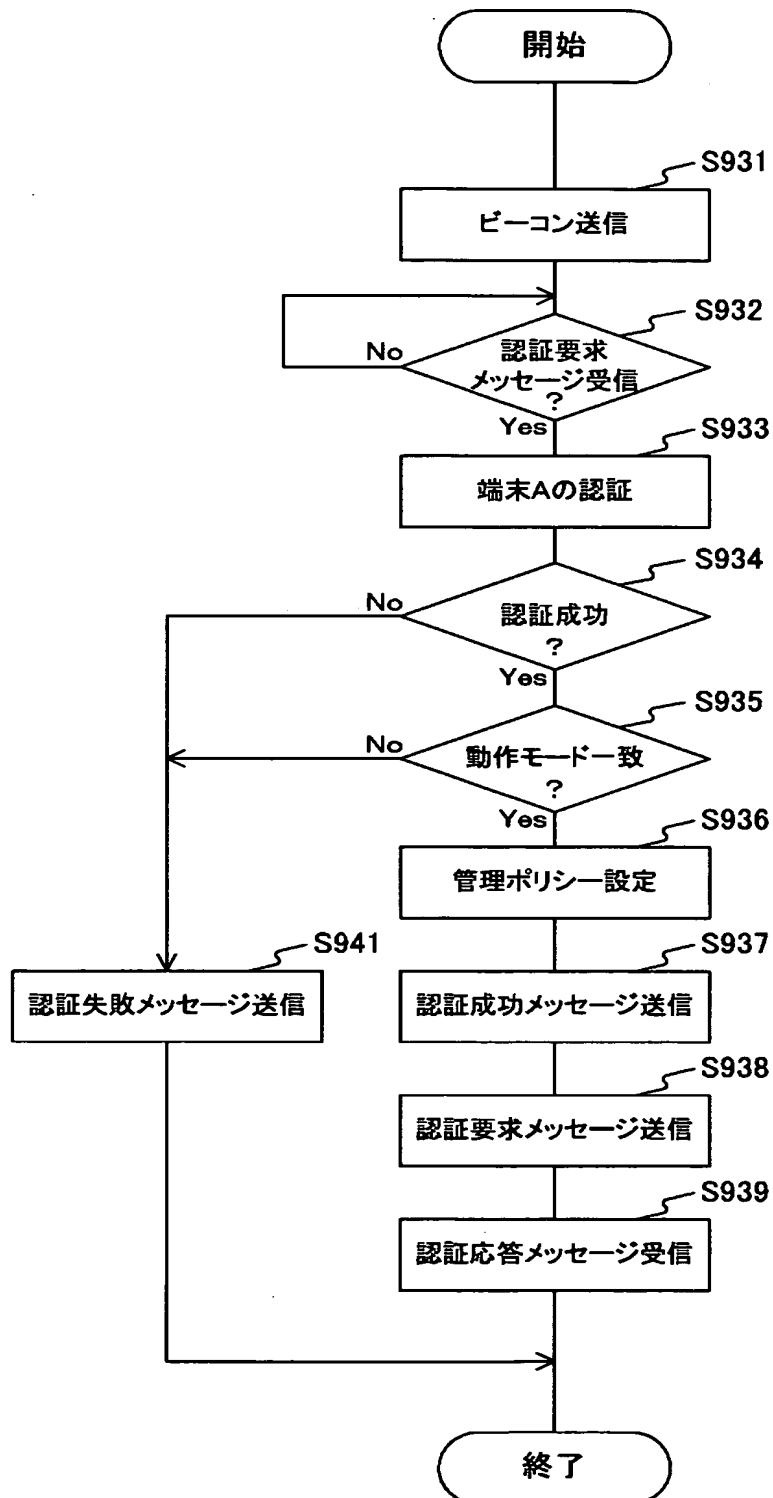
【図 11】



【図 12】



【図 13】



【書類名】 要約書

【要約】

【課題】 無線通信システムのネットワークに接続しようとする端末において接続対象のネットワークを識別させ、または、接続対象のネットワークにおける権限を提示させる。

【解決手段】 ネットワークに参入しようとする端末B（200）は、ネットワーク識別子および動作モードを含むビーコン2011を送信（201）する。ネットワーク識別子は、端末Bがネットワークに接続するために使用する属性証明書の発行端末の端末識別子を用いることができる。動作モードは、端末Bが動作するモードである。ビーコン2011を受信した端末A（100）は、端末A自身が動作するモードとビーコン2011に含まれる動作モードとが合致することを確認（102）する。そして、端末Aは、ビーコン2011に含まれるネットワーク識別子と合致する属性証明書を提示して端末Bに対して認証要求（111）を行う。

【選択図】 図10



特願 2 0 0 3 - 0 5 9 3 5 9

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 2 1 8 5]

1. 変更年月日

1 9 9 0 年 8 月 3 0 日

[変更理由]

新規登録

住 所

東京都品川区北品川 6 丁目 7 番 3 5 号

氏 名

ソニー株式会社